Securing Embedded Devices

Hassan Fallah-Adl
Senior Staff Architect
Intel Corporation

Legal Disclaimer

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Intel® Insider™ is a hardware-based content protection mechanism. Requires a 2nd generation Intel® Core™ processor-based PC with built-in visuals enabled, an Internet connection, and content purchase or rental from qualified providers. Intel® Insider™ requires an HDCP protected display. VGA output not supported. Consult your PC manufacturer. For more information, visit www.intel.com/go/intelinsider.

Intel® Active Management Technology: Requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup & configuration. For more information, visit www.intel.com/technology/platform-technology/intel-amt

Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: www.intel.com/technology/vpro

Intel® Trusted Execution Technology: No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit www.intel.com/technology/security

Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/go/virtualization

No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware and software and a subscription with a capable Service Provider. Consult your system manufacturer and Service Provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit http://www.intel.com/go/anti-theft

*Other names and brands may be claimed as the property of others.

Security For Embedded Markets

Embedded represents a complex ecosystem of regulations, technologies and realities

Security Threats are increasing for Embedded Devices

Security has emerged as a key platform value

- Regulations, compliancy are changing the security, privacy and safety landscape for embedded systems
- Security awareness and design must grow

Security will continue to define opportunity for growth and innovation in embedded systems

intel

Increasing Embedded Device Security Threats

Pentagon: Y

acknowled
mess left

Stuxnet Cyberattack on Iran Arms Hackers with New Ideas

Oct 11, 2010 | 5:53 PM ET | By Stuart Fox, SecurityNewsDaily Staff Writer

has admitted
security brea
as "the most

Security researchers hac

Water treatment plant hacked

Hacking the Car: Cyber Security Risks Hit the Road

By Josie Garthwaite | Mar. 19, 2010, 12:00am PDT | 8 Comments

Experts hack power grid in no time

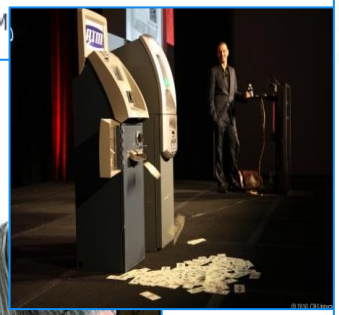
Basic social engineering and browser exploits expose electric producti

Security researchers to unveil pacemaker, medical implant hacks

st of your friends.

'Smart' utility meters have security h
be hacked, expert finds

Published: Friday, March 26, 2010, 3:31 PM



Water Canal Syste

Wednesday, March 26, 2008

Clear Channel electronic billboards get hacked UPDATE: no they didn't, maybe

Cra
see
wor
cou
mal
batt
ever
Tex
with

Industrial virus revives power grid hacking fears

Safety of power plants and distribution in question

By Jaikumar Vijayan | Computerworld US

Published: 10:05 GMT, 27 July 10

Last week's disclosure of a sophisticated malware program targeting control system software from Siemens AG has renewed long-standing

Her
the
a ca
into

August 31, 2010 11:07 AM PDT

Cars: The next hacking frontier?

veiled a program
re, including the
led "Perfect Citiz
geared to bring attention to the possibility of grid hacking

havoc on more than 100

, 2010 | 04:47 PM

ly Jackson Higgins

DarkReading

Introducing: Experimental Security Panorama (ESP) Workshop

intel

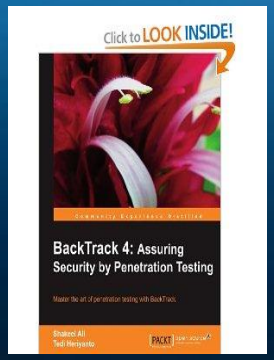
“How to” guides abound for hacking embedded device h/w

With physical access to the h/w, hackers attempt to: (examples)

- Read JTAG info to learn vulnerabilities
- Extract and decompile from ROMs initialization code, steal keys, learn configuration options
- Redirect boot to infected local sources (e.g. CD, USB)

With remote access to h/w, hackers attempt to: (examples)

- Redirect boot to infected remote sources (e.g. image on internet)
- Subvert management interfaces to gain supervisor privilege
- Subvert firmware patching processes to revert to older vulnerable versions of firmware (e.g. BIOS)



Embedded systems are no longer protected by ignorance or isolated networks

Protecting against S/W attacks

With connected access to the s/w, hackers attempt to disrupt device operation by: (examples)

- Unauthorized login/access
- Malformed network packets or expected I/O data
- Denial of service attacks
- System resets

With remote access to s/w, hackers attempt to: (examples)

- Reconfigure policies, configurations and steal keys
- Manipulate behavior in an attempt to disrupt and possibly destroy device
- Subvert patching processes to replace known good applications with malware

Embedded devices are under attack with hundreds of examples highlighted within the news daily

intel

Embedded System Challenges

Maintaining Security and Control Across the Lifecycle

Device Manufacturer	Distributor/Dealer	Device Owner

- Patching
- Problem/Resolution
- Change Control

- Customization
- Support
- Patching

- Compliance
- Performance
- Manageability

Security, Control, & Compliance

Driving Security Into Embedded Systems

Create security awareness in embedded system design and deployment

Delivering successful security features affects the entire product lifecycle from product design to deployment to end of life

- Security must be designed into products
- The underlying technologies matter
- The *human factor* **cannot** be disregarded

A well managed system is a secure system

intel

Security Innovation with Intel® Core™ Processors

Creating more secure products using Intel Technology

- Intel® Anti Theft Technology
- Intel® Trusted Execution Technology
- Intel® Advanced Encryption Standard New Instructions
- Intel® Digital Random Number Generator

Intel security technologies leverage hardware protections

Intel continues to support and drive security standards and policy

Increase the security, privacy and reliability of embedded systems with Intel® Core™ Processors*

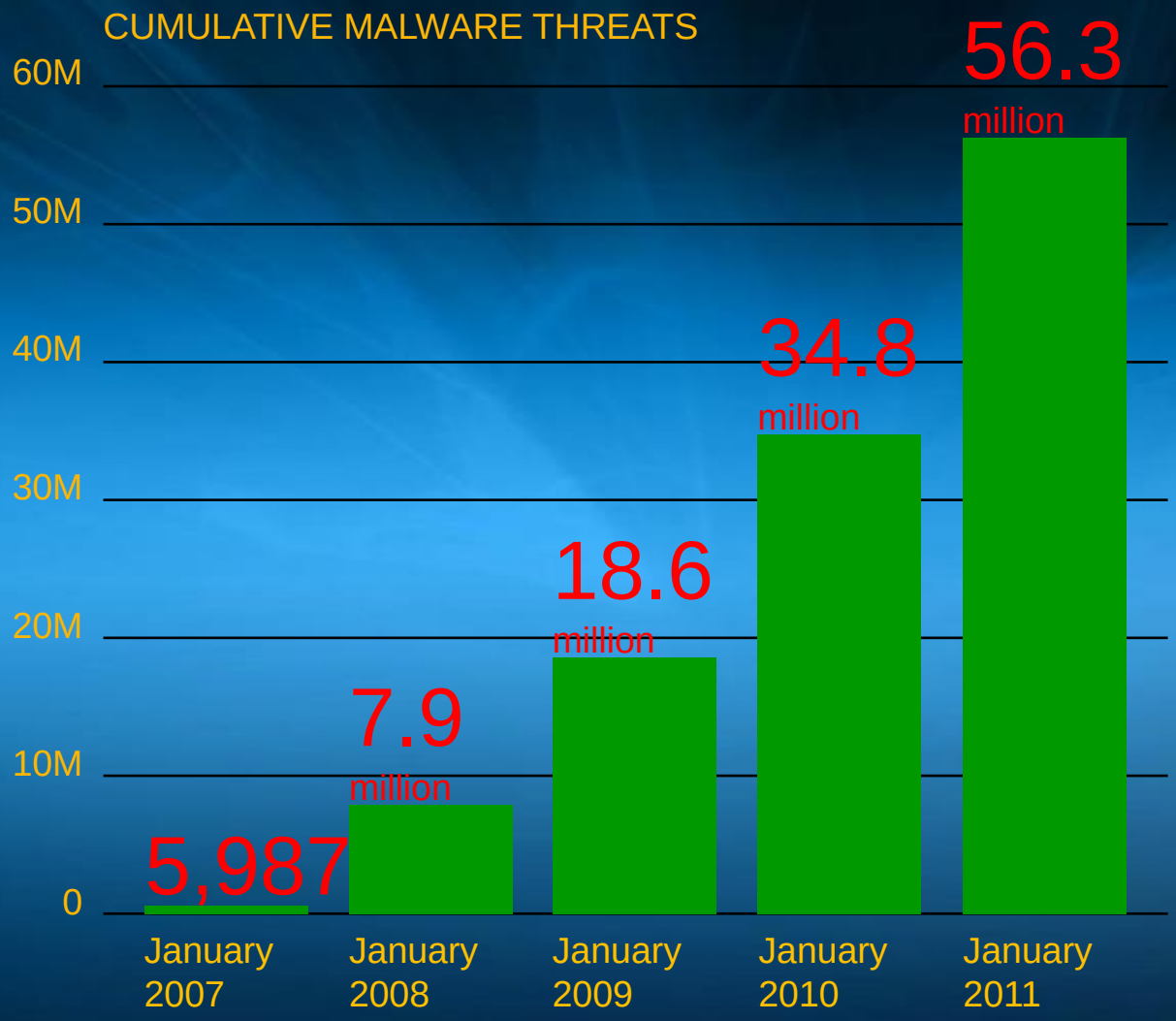
* 1st and/or 2nd generation Intel® Core based processors

BACKUP


Introducing:
Experimental
Security Panoramas
(ESP) Workshop

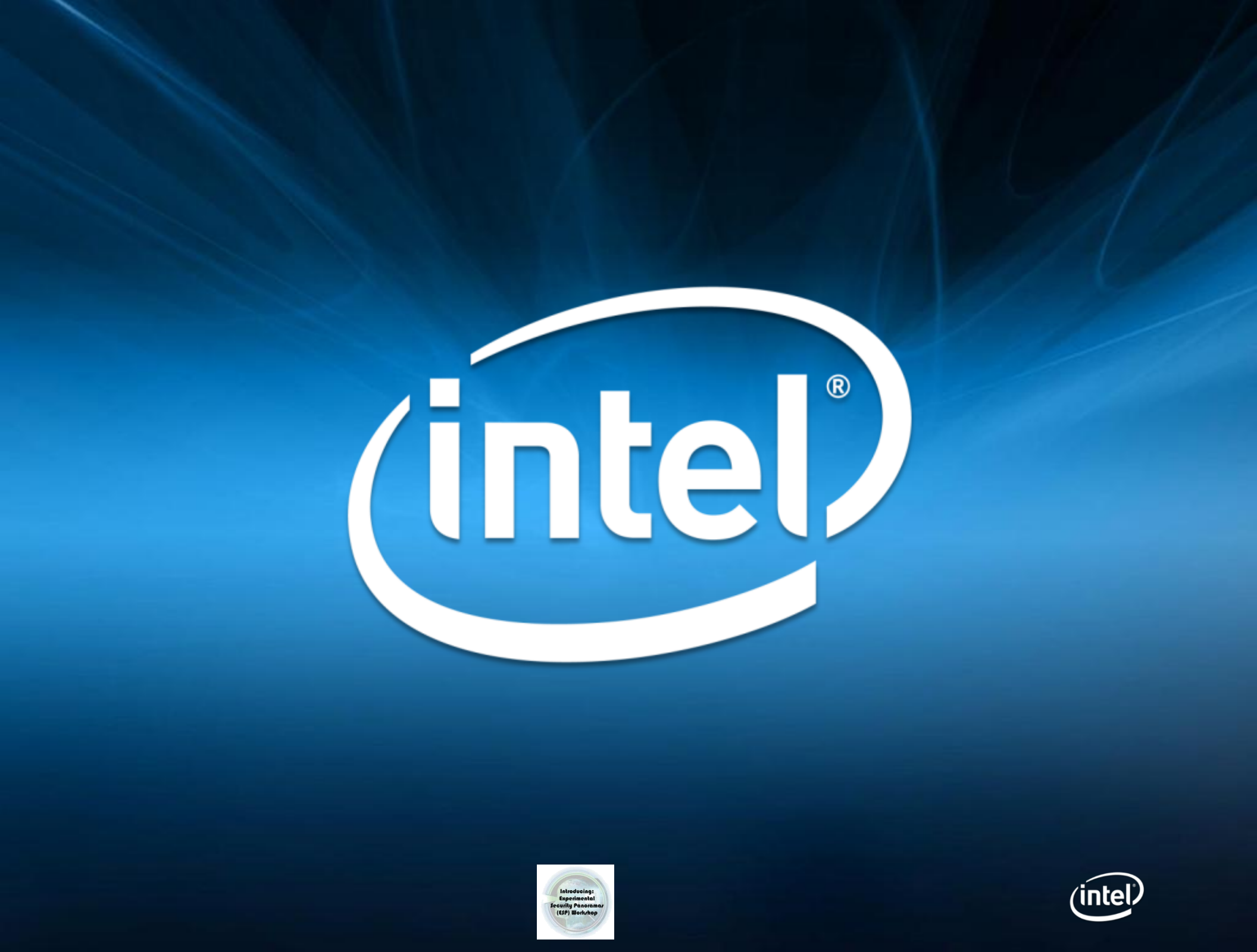

intel

Unprecedented Malware Growth



Source: McAfee Labs

Introducing: Experimental Security Panoramas (ESP) Workshop


intel
Introducing:
Experimental
Security Panoramas
(ESP) Workshop
intel